## REMARKS

Claims 1 and 4-21 are now pending. Reconsideration is respectfully requested.

**35 U.S.C. § 103 Rejections**

Claims 1, 4-5, 8-13, 15-18, and 20-21 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Wentker et al. (U.S. Patent No. 6,481,632) and further in view of Muttik et al. (U.S. Patent No. 6,907,396). Applicant respectfully traverses this rejection.

The Wentker-Muttik combination does not teach or suggest each and every element of the claims. Newly cited Wentker has no relevance to the present invention as claimed. In any instance, Applicant respectfully submits that construction of the claim language is unreasonably broad. While the claims are to be given the broadest reasonable construction, the broadest reasonable construction is one "read in the appropriate context of the claim language and specification. *In re Suitco Surface, Inc.*, 2009-1418 (Fed. Cir. 2010). In order for Wentker to be remotely applicable to the claims at hand, the claims have to be read out of their specific context as provided by the instant specification.

Wentker's invention is specifically applicable to smart cards. Wentker's invention enables an issuer of a smart card, for example, a credit card company, to provide limited management capabilities (i.e., delegated management) to application provides to load, install, and delete a their application on the smart card. These changes are pre-approved by the smart card issuer to increase the flexibility in managing the smart card. In this system, the application provider may prevent the issuer from accessing private user data on the card because they are delegated separate security domains to manage their application. The issuer can simply pre-approve certain applications by providing a command authentication pattern to the application provider. Upon loading an application on a smart card, the command authentication pattern is verified. See e.g., col. 2, line 65 – col. 3, line 40.

The present invention as claimed utilizes a validator program that scans and validates software by running the software in an emulator in a secure environment. The secure environment comprises a modified operating system for the emulator to run in so that the code may be examined for malicious routines such as viruses, Trojans and the like.

It is unclear how Wentker can be analogous to the present invention as claimed. The examiner states that "upon loading the software on the open platform computer system, initiating a pre-synchronization scan" and "during the pre-synchronization scan, validating the software by the use of a validator program residing in the open platform computer system in a secure fashion such that the validator program scans the software that is loaded in the secure environment" is equivalent to, respectively:

> The card issuer pre-authorizes the initial install command (which performs loading) and the load file through the use of these data authentication patterns. The data authentication pattern for the application file is included in the initial Install command to ensure that application which has been approved by the card issuer is the same application that is subsequently received by the card manager through the series of loading commands that follow the first install command. Col. 12, lines 49 – 57.

and

> Testing of an application for a smart card may be performed in any of a variety of ways and is a step understood in the art, and generally involves functional tests (optional) and security tests (mandatory). Testing of the application involves checking its operational behavior on a smart card, checking its operational memory requirements, etc., ensuring that the application is secure, and checking for viruses and card related threats. Once the issuer (or trusted third party) has tested the application and it to ensure that it behaves correctly, the application is "certified" and the issuer is ready to prepare the application for a delegated load and installation by the provider. Col. 15, lines 8 – 19.

Applicant disagrees. Neither citation references a pre-synchronization scan, a validator program, an emulator, or scanning software the software by the validator program in a secure environment. With respect to these passages, Wentker's disclosure has absolutely no relevance to the claims at hand. These citations are within a section describing Fig. 7A, which is a flow diagram describing a technique for delegated loading. Wentker describes delegated loading as "allow[ing] the application provider to establish a loading session for transferring their application files directly to their own security domains." Col. 12, lines 29 – 31. The data authentication pattern is merely a mechanism used to ensure the authenticity of the software. In other words, to ensure that the software approved by the issuer is the same software being loaded.

Notwithstanding the fact that Wentker contains no concept of a pre-synchronization scan, at no time is the software to be loaded scanned or validated during a pre-synchronization scan by an emulator. The testing referred to in the above citation merely states that an issuer may have a third party test an application on a smart card to make sure it runs properly. This testing step is divorced from any process related to Wentker's invention, but is merely an acknowledgement by the inventor that the software industry generally tests its software before distribution. Even if this testing could be construed as being relevant disclosure as the examiner asserts, there is no mention of running an emulator in a modified operating system so that the code may be examined for malicious routines as claimed.

Furthermore, the above passage does not state that the software is marked with a flag during any validation process that would possibly deny the software the ability to run on the system and deny synchronization. Again, notwithstanding that Wentker does not disclose a synchronization process, if the software would be tested by a third party and would not meet the issuer's specifications, it is likely that the software would be fixed by the application provider so that the software would run. There would be no conceivable reason for a third party to test a piece of software only to mark the software as unusable and still enable it to be distributed to the issuer for use on a smart card. Given the context of Wentker's disclosure, this scenario tests the limits of reasonableness.

Next, the examiner states that "automatically denying the software the ability to operate on any environment within the open platform computer system and denying synchronization of the software with the portable computer device if the validator fails to identify said software as valid in order to ensure the security of the open platform computer system" is equivalent to the Card Manager Locked state as described by Wentker (see col. 9, lines 34 – 65). Applicant respectfully submits that this is an example of the examiner merely finding single functionality (or corollaries) within Wentker and applying such functionality to the claims with little or no regard to the context of such functionality.

Wentker describes a card manager that is able to disable all applications on a card so that the issuer may inspect the card to detect threats. While in this state, the card does not function. While this does deny software on the card to run, this functionality is in no way connected to a validation program that employed an emulator to detect malicious code right before

synchronization. When read within context of the specification, the card manager is software that allows an issuer to manage the lifecycle of the card. See e.g., col. 8, line 40 – col. 11, line 12. In other words, the card manager software can be used to set the card in a variety of states. One state enables the security domains and key sets to be loaded on the card. See e.g., col. 9, lines 5 – 12. The Secured state is the normal operating state of the card. See e.g., col. 9, lines 13 – 32. Another state, the Terminated state, enables the issuer to disable the card completely (the equivalent of someone cutting a traditionally credit card in half). None of these states are activated during a pre-synchronization or synchronization process. None of these states work in conjunction with a validator program to prevent malicious code from being propagated during synchronization. Notwithstanding Wentker has no concept of a synchronization process, Wentker provides no disclosure of validating software as one process prior to a synchronization.

The suggest combination of Wentker with Muttik is improper. Wentker provides absolutely no motivation, teaching, or suggestion for one ordinarily skilled in the art to consult Muttik (or any reference discussing emulator's for that matter). Muttik teaches improving an already existing emulator by patching additional instructions (i.e., extensions) into the emulator. See e.g., Abstract, col. 1, lines 46 – 50, and col. 2, lines 10 – 15. Muttik does not discuss situations where an emulator would be advantageous or disadvantageous as emulators existing before Muttik. Muttik's invention assumes that an emulator on a system exists and that using extensions is an improvement to that security technique. So any suggestion that emulation would be a valuable technique to combine with Wentker comes solely, and impermissibly, from the Applicant's disclosure.

Furthermore, Muttik's scope does not include and thus does not disclose "a computer system comprising a host facility and a portable computer device coupled to the host facility" (emphasis added). In other words, like Wentker, Muttik has no concept of a synchronization process and the challenges faced by the use of such a process. Muttik is directed to a single system performing its functionality. See, e.g., col. 3, lines 43-49. Muttik does not disclose a system wherein a host and a portable device are operating in concert to achieve the claimed functionality. So any combination with Wentker must come from the Applicant's disclosure.

So to combine Muttik with Wentker, the disclosed smart card process would need to be modified to include an emulator. Wentker does not discuss or even recognize the issue of

emulating (even when discussing testing procedures). Neither reference discloses a pre-synchronization or synchronization process so neither reference is capable of disclosing denying a synchronization of software. Wentker and Muttik, alone or in combination, do not disclose, teach, or suggest each and every element of the claims as required. As argued above, one ordinarily skilled in the art would not look to combine these references because of their quite disparate teachings. Accordingly, Applicant respectfully requests withdrawal of this rejection.

Claim 7 stands rejected under 35 U.S.C. § 103(a) as unpatentable over Wentker and Muttik as applied to claim 1, and further in view of Brody et al. (U.S. Pub. No. 2001/0051928). Applicant respectfully traverses this rejection.

As argued with regard to claims 1, Wentker and Muttik, alone or in combination, do not teach or suggest the present claims. Brody does not cure the Wentker-Muttik combination's deficiencies. As argued in previous responses, it is unclear how Brody has any relevance to Muttik and now it is equally unclear how Brody has any relevance to Wentker. Brody adds nothing to the combination and as such the combination still does not teach or suggest the claim. Any motivation to combine these references comes solely from the Applicant's disclosure. Accordingly, Applicant respectfully requests withdrawal of this rejection.

Claims 6, 14, and 19 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Wentker and Muttik as applied to claims 1, 8, & 18, further in view of Ginter et al. (U.S. Patent No. 6,948,070). Applicant respectfully traverses this rejection.

As argued with regard to claims 1, 8, and 18, Wentker and Muttik, alone or in combination, do not teach or suggest the present claims. Ginter does not cure the Wentker-Muttik combination's deficiencies. Ginter is directed towards electronic commerce transactions and has little or no relevance to either Wentker or Muttik. Any motivation to combine these references comes solely from the Applicant's disclosure. Accordingly, Applicant respectfully requests withdrawal of this rejection.

**CONCLUSION**

In light of the above remarks, Applicant respectfully requests reconsideration of the rejected claims and solicits their allowance. In the event an interview is useful in resolving any issues, the examiner is invited to telephone the undersigned representative.

Respectfully submitted,

BERRY & ASSOCIATES P.C.

Dated: November 30, 2010

By: /Shawn Diedtrich/
Shawn Diedtrich
Registration No. 58,176
Direct: 480.704.4615

9229 Sunset Blvd., Suite 630
Los Angeles, CA 90069
(310) 247-2860